CyberVolk Ransomware: Analysis of Double Encryption Structure and Disguised Decryption Logic

⋮ 9/8/2025

Malware

- Sep 09 2025

The CyberVolk ransomware, which first emerged in May 2024, has been launching attacks on public institutions and key infrastructures of various countries, posing a continuous threat. The ransomware is particularly notable for its pro-Russia nature, as it primarily targets anti-Russian countries, making it a geopolitically significant cyber threat. This post provides a technical analysis of the internal workings, encryption structure, and reasons why decryption is not possible in order to offer insights for preparing against similar threats in the future.

1. CyberVolk Ransomware Group

CyberVolk is a ransomware group that emerged in May 2024. It is believed to be pro-Russia and targets public institutions of countries deemed hostile to Russia’s interests. The group recently claimed to have

attacked major infrastructure facilities and scientific institutions in Japan, France, and the UK. The group uses Telegram as its main communication channel.

Figure 1. CyberVolk group logo

2. Analysis Details

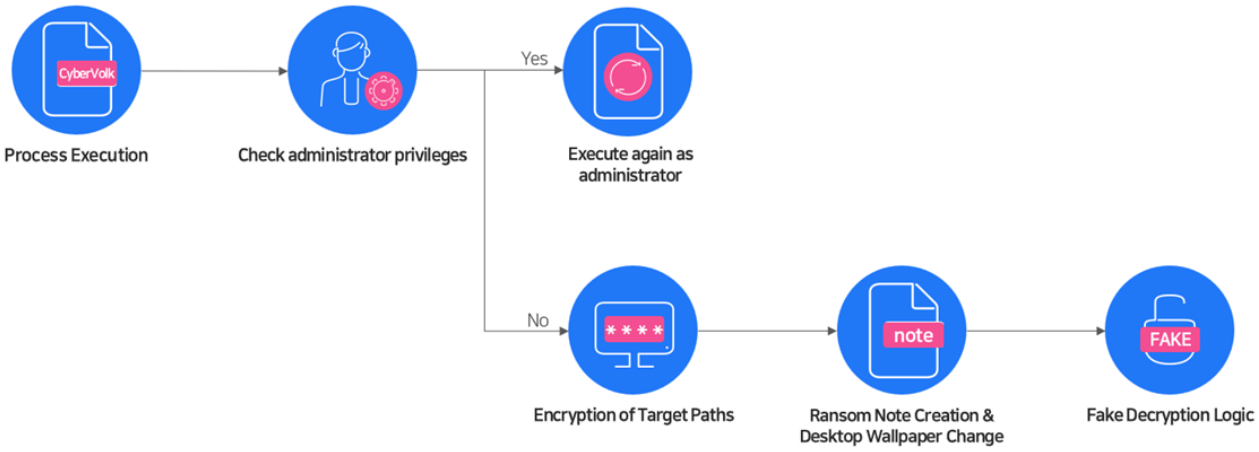

Figure 2. CyberVolk execution flow

When the CyberVolk ransomware is initially executed with normal user privileges, it restarts the ransomware with administrator privileges. It excludes certain items from encryption, such as files and directories that may

cause issues in the system when encrypted. It also excludes encryption targets that contain the strings shown in Table 1 in their paths or filenames. For the excluded extensions, the CyberVolk ransomware encrypts files without distinguishing the extension, except for the extension that is changed during encryption. This prevents re-encrypting files that are already encrypted.

Strings related to encryption exclusion targets
Windows
Program Files
ProgramData

Table 1. Strings related to exclusion from encryption

Extensions Excluded from Encryption
.CyberVolk

Table 2. Extensions excluded from encryption

The algorithms used for encryption are the symmetric key encryption methods AES and ChaCha20-Poly1305. The key used for encryption is generated before the main function starts, and all files are encrypted using the same symmetric key.

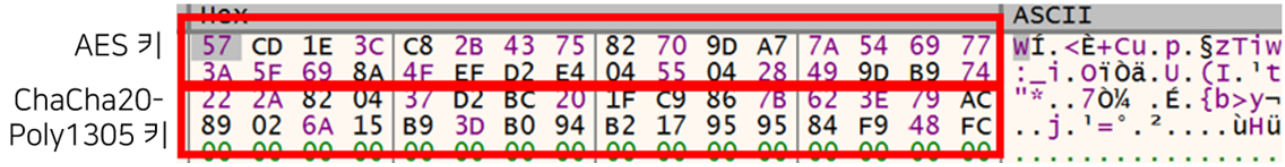

Figure 3. Symmetric key used in the encryption algorithm

During encryption, a 12-byte random value known as a nonce (number used once) is generated using the crypto_rand_Read() function. The nonce is a unique, one-time value that prevents the encryption algorithm from producing the same output for the same input. The file content is then encrypted using AES-256 GCM mode. The encrypted file content is then further encrypted using ChaCha20-Poly1305.

```
File = os_ReadFile(a1, a2, a3, a4, a5, a6, a7, a8, a9);
if ( a4 )
  return a4;
v80 = File;
v15 = crypto_aes_NewCipher((unsigned int)&xmmword_9FDA20, 32, 32, 0, a5, v11, v12, v13, v14, v51, v60);
v76 = crypto_cipher_NewGCM(v15, 32, v16, 0, a5, v17, v18, v19, v20, v52, v61);
v75 = (*(__int64 (__golang **)(__int64))(v76 + 24))(32);
v82 = runtime_makeslice((unsigned int)&RTYPE_uint8, v75, v75, 0, a5, v21, v22, v23, v24, v53, v62);
crypto_rand_Read(v82, v75, v75, 0, a5, v25, v26, v27, v28, v54, v63);
v29 = v82;
v81 = (*(__int64 (__golang **)(__int64, _QWORD, _QWORD, _QWORD, __int64, __int64, __int64))(v76 + 48))(
        32,                                     // crypto_internal_fips140_aes_gcm__ptr_GCM_Seal
        0,
        0,
        0,
        v82,
        v75,
        v75);
```

Figure 4. Encryption with AES-256 GCM mode

Upon examining the structure of the encrypted file as described above, only the encrypted file content and the authentication tag generated by the ChaCha20-Poly1305 encryption are present.

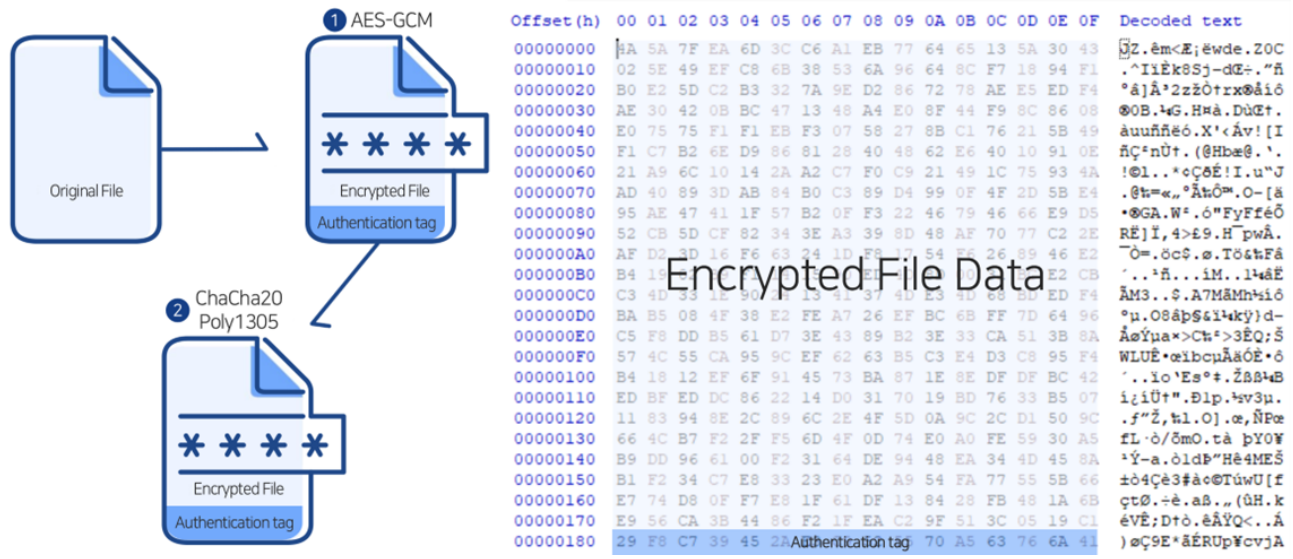

Figure 5. Structural changes between the original file and the encrypted file

The ransom note is named READMENOW.txt, and it is only created in the path where the CyberVolk ransomware is executed after file encryption is completed.

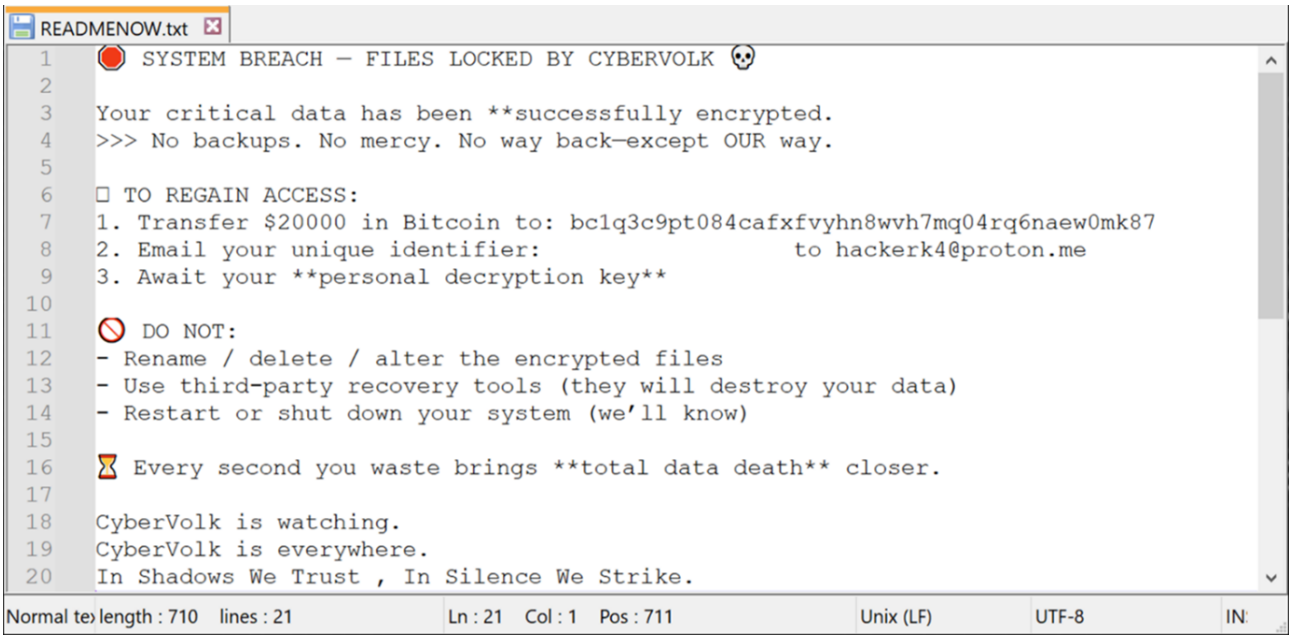

Figure 6. The created ransom note

After changing the desktop background and running the ransom note, a message is displayed in the prompt window, saying that the files have been encrypted and users have three attempts to enter the decryption key. The decryption key is hard-coded into the file, and entering the correct key triggers the decryption logic.

First, an attempt is made to decrypt the contents of the file encrypted with ChaCha20-Poly1305. However, there is an issue with this process, and the decryption is not successful. During decryption, the correct Nonce value used in encryption must be used. However, an incorrect Nonce value is used in this case, causing the decryption to fail.

Figure 7. Decryption of the file

3. Conclusion

The CyberVolk ransomware group first emerged in May 2024 and has a pro-Russian inclination. They target public agencies of countries with a pro-Russian inclination and inflict damages by using their own ransomware variants. As described in this report, the ransomware uses the SHA-256 algorithm to encrypt a string that is hard-coded in the file, and this encrypted value is used as a symmetric key. The file content is then encrypted with the AES and ChaCha20-Poly1305 algorithms.

The nonce value used for encryption is different for each file and is generated randomly. However, since this value is not stored in the encrypted file, it cannot be decrypted. In response to this incident, companies are advised to back up important data to an offsite location separated from the service network to protect and operate key assets securely. They should also implement access controls for the backup repository and conduct regular recovery drills. It is essential to take strategic measures to ensure the security and recoverability of the backup system, going beyond simple data backup.

4. AhnLab’s Response

4.1. V3

Ransomware/Win.BlackLock.C5764855 (2025.06.11.03)

Ransom/MDP.Behavior.M2649 (2022.09.06.00)

Ransom/MDP.Decoy.M1171 (2016.07.15.02)

4.2. EDR

Ransom/EDR.Decoy.M2716 (2025.08.07.00)

MD5

c04e70613fcf916e27bd653f38149f71

Additional IOCs are available on AhnLab TIP.